In the Claims:

Please amend claims 1-21 as follows:

1. (Currently Amended) A storing apparatus for use with a computer-based system in which a first user can protect access to information recorded on a medium with a second password, and can selectively permit said first user and a second user to access the information without the second password, comprising:

a password preserving unit for preserving a first ~~general access~~ password and the second password; and

a password verifying unit which, when an access authorization is requested by entering a password, compares the entered password with the second password; if in agreement, issues an authorization, and if not, refuses to issue an authorization;

and when an access authorization is requested without entering a password, compares the first password and the second password; if in agreement, issues an authorization, and if not, refuses to issue an authorization.~~a password verifying unit for allowing access if the password is entered, and if the password is not entered, comparing the general access password with the password, allowing access if the general access password is the password, and denying access if the general access password is not the password.~~

2. (Currently Amended) An apparatus according to claim 1, wherein in the case where a same value has been preserved in the first~~general access~~ password and the

second password for access protection by said password preserving unit, even if there is no user input password input by the user, said password verifying unit permits an access by substituting said firstgeneral access password for the user input password and comparing the firstgeneral access password with the second password for access protection.

3. (Currently Amended) An apparatus according to claim 1, wherein

said password preserving unit further has a user input password area to store a user input password input by a user, and

said password verifying unit is constructed in a manner such that

at the start of the use of the apparatus such as turn-on of a power source, command reset, error reset, medium insertion, or the like, said firstgeneral access password is read out and written into said user input password area, an access permission is established if the firstgeneral password is the password, or an access inhibition is established if the firstgeneral password is not the password, on the basis of a collation between the firstgeneral access password in said user input password area and the second password for access protection,

after said access permission or inhibition is established, each time there is a password input of the user, the user input password is written into said user input password area and, subsequently, the access permission inhibition is established on the basis

of a collation between the user input password in said user input password area and the second password for access protection.

4. (Currently Amended) An apparatus according to claim 1, wherein

said password preserving unit further has a user input password area to store a user input password input by a user, and

said password verifying unit is constructed in a manner such that

at the start of the use of the apparatus such as turn-on of a power source, command reset, error reset, medium insertion, or the like, the apparatus waits for the password input by the user in a state where said first~~general access~~ password is read out and written into said user input password area, when there is the user password input, the user input password is overwritten into the first~~general access~~ password in said user input password area, and after that, the password in said user input password area and said password for access protection are compared and the access protection is controlled, and

when there is no user password input and/or in the case where the password is an empty character train even if there is the user password input, the comparison between the first~~general access~~ password in said user input password area and the second password for access protection is executed and the access protection is controlled.

5. (Currently Amended) An apparatus according to claim 1, wherein said password preserving unit preserves said first~~general access~~ password and said second password for access protection into a non-volatile memory of an apparatus main body.

6. (Currently Amended) An apparatus according to claim 1, wherein

said password preserving unit preserves said first~~general access~~ password and said second password for access protection into said medium, and

said password verifying unit reads out said first~~general access~~ password and said second password for access protection from said medium and stores into an apparatus main body at the start of the use of the apparatus and controls the access protection.

7. (Currently Amended) An apparatus according to claim 1, wherein

said password preserving unit preserves said first~~general access~~ password into a non-volatile memory of an apparatus main body and preserves said second password for access protection into the medium, and

said password verifying unit reads out said second password for access protection from said medium and stores into the apparatus main body at the start of the use of the apparatus and controls the access protection.

8. (Currently Amended) An apparatus according to claim 1, wherein said password preserving unit preserves said second password for access protection into a non-volatile memory of an apparatus main body and preserves said first~~general access~~ password into the medium, and

said password verifying unit reads out said first ~~general access~~ password from said medium and stores into the apparatus main body at the start of the use of the apparatus and controls the access protection.

9. (Currently Amended) An apparatus according to claim 1, wherein in said medium, a password preserving area to preserve said second password is provided in a specific area which cannot be accessed by an ordinary read command and write command.

10. (Currently amended) An apparatus according to claim 1, further comprising a password rewriting unit for rewriting said default input password or said first password for access protection on the basis of a dedicated command from an upper apparatus.

11. (Original) An apparatus according to claim 1, wherein said medium is a medium fixedly enclosed in the apparatus main body.

12. (Original) An apparatus according to claim 1, wherein said medium is a removable medium which is detachable from the apparatus main body.

13. (Currently amended) An apparatus according to claim 1, wherein

said password preserving unit preserves a plurality of kinds of passwords for access protection according to kinds of access protection, and

said password verifying unit permits an access by an ordinary command corresponding to the kind of said first password for access protection in which a collation coincidence is obtained.

14. (Currently amended) An apparatus according to claim 13, wherein

as said first passwords for access protection, said password preserving unit preserves a write/read password to permit an access by a read command and a write command and a read only password to permit only an access by the read command, and

said password verifying unit permits the access by the ordinary write command or read command when the collation coincidence of said write/read password is obtained and permits the access by only the ordinary read command when the collation coincidence of said read only password is obtained.

15. (Currently Amended) An apparatus according to claim 1, further comprising a validity term setting unit for setting a validity term into said firstgeneral access password.

16. (Currently Amended) An apparatus according to claim 15, wherein said validity term setting unit counts the number of using times of the apparatus by a counter and, when a value of said counter reaches a predetermined value, said validity term setting unit forcedly changes said firstgeneral access password to a value different from the firstgeneral access password so far.

17. (Currently Amended) An apparatus according to claim 15, wherein said validity term setting unit sets a time of a validity term and, when a present time in case of using the apparatus exceeds said validity term, said validity term setting unit forcedly changes said firstgeneral access password to a value different from the firstgeneral access password so far.

18. (Currently Amended) A method of protecting access to information recorded on a medium with a second password for use with a computer-based system, comprising:

a password preserving step of preserving the password and a first ~~general access~~ password; and

a password verifying step which, when an access authorization is requested by entering a password, compares the entered password with the second password; if in agreement, issues an authorization, and if not, refuses to issue an authorization;

and when an access authorization is requested without entering a password, compares the first password and the second password; if in agreement, issues an authorization, and if not, refuses to issue an authorization.~~of controlling the access protection by comparing a user input password input by a user with the password when there is the user input password, allowing access if the user input password is the password, and denying access if the user input password is not the password, and for controlling access protection by comparing said general access password substituted for said user input password with the password when there is no user input password, allowing access if said general access password is the password, and denying access if said general access password is not the password.~~

19. (Currently Amended) A method according to claim 18, wherein in the case where a same value has been preserved in said first~~general access~~ password and said second password for access protection, in said password verifying step, prior to the password input of the user, a value of said first~~general access~~ password is copied to the user input

password and is collated with said second password for access protection, thereby permitting or inhibiting an access.

20. (Currently Amended) A method according to claim 18, wherein

in said password preserving step, a plurality of kinds of passwords for access protection according to kinds of said access protection are preserved, and

in said password verifying step, an access by an ordinary command corresponding to the kind of said first password for access protection in which a collation coincidence is obtained is permitted.

21. (Amended) A method according to claim 18, further comprising a validity term setting step of setting a validity term into said first~~general access~~ password.

password and is collated with said second password for access protection, thereby permitting or inhibiting an access.

21. (Amended) A method according to claim 18, further comprising a validity term setting step of setting a validity term into said first~~general access~~ password.